



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools
and Universities\)](#)

[International](#)

[Information Technology and
Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security
Contacts](#)

[Emergency Services](#)

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

(Minnesota) Hacker charged over siphoning off funds meant for software devs. An alleged hacker has been charged with breaking into the e-commerce systems of Digital River before redirecting more than \$250,000 to an account under his control. The hacker, of Houston, Texas, 35, is charged with fraudulently obtaining more than \$274K between December 2008 and October 2009 following an alleged hack against the network of SWReg Inc, a Digital River subsidiary. SWReg specializes in running e-commerce fulfillment systems for smaller software developers who do not want the hassle of developing and maintaining their own online store. An indictment in the case, filed in a federal court in Minnesota, was unsealed December 21. A separate computer intrusion earlier this year obliged Digital River to obtain a court order against an individual who was allegedly planning to sell 200,000 records from a stolen database, net security firm Sophos notes. Source:

http://www.theregister.co.uk/2010/12/23/digital_river_hack_charges/

(Minnesota) Most wastewater violations go unpunished. Most violations of federal clean water standards in Minnesota go without any punishment, and most of the state's major industries have violated rules in recent years. That is the finding of a report released December 20 by the Minnesota Center for Environmental Advocacy. Among the 11 most frequent violators in Minnesota, five are in the Northland, including Boise White Paper in International Falls (sediments and oxygen levels), Minnesota's Power's Laskin Energy Center in Hoyt Lakes (warm water), Boswell Energy Center in Cohasset (chlorine, copper and sediment) and North Shore Mining Co. operations in Silver Bay (fluoride and fibers), and Babbitt (oxygen levels, chlorine, iron, nitrogen, ammonia and sediments). Statewide, the plants in noncompliance exceeded limits for several pollutants — including fecal coliform, phosphorus, chlorine, copper and mercury — all known to harm human and aquatic health at elevated levels. The report looked at 5 years of compliance reports from the Minnesota Pollution Control Agency and found only 11 percent of the violations brought any penalty for polluting beyond federal rules. The audit also found two-thirds of the factories, sewage treatment plants and other facilities that release discharge into public waters had at least one violation. For large industrial plants, the violation rate was 88 percent. "These aren't complicated cases. These are reported violations, they are serious violations, and yet 9 out of 10 lawbreakers who turn themselves in get by without a fine," said the report's author. It found 356 of the total 1,287 permitted facilities across Minnesota were in "significant noncompliance" at some point over the 5 years. Source:

<http://www.duluthnewstribune.com/event/article/id/186883/>

(Montana) EPA orders oil companies to monitor public water supply and private wells in Poplar, Montana. In response to recent detections of low levels of oil production-related contaminants in the public water supply that serves Poplar, Montana, and the Fort Peck Indian Reservation, the U.S.

UNCLASSIFIED

Environmental Protection Agency (EPA) December 16 issued an order to Murphy Exploration & Production Co. (Murphy), Pioneer Natural Resources USA, Inc. (Pioneer), and Samson Hydrocarbons Co. (Samson). EPA's order, issued under the Safe Drinking Water Act, requires the companies to monitor Poplar's water supply wells, and also the private wells of residents in the potentially affected area, upon resident request. The order also requires the companies to provide additional water treatment and/or alternate supplies if EPA determines the groundwater in wells is becoming a public health risk. Murphy, Pioneer and Samson are, directly or through corporate acquisition, historic oil producers in the East Poplar oil field. The field has many known contaminated groundwater plumes caused by past production practices. Source:

<http://yosemite.epa.gov/opa/admpress.nsf/e77fdd4f5afd88a3852576b3005a604f/c8029d6c7f6f0b4e852577fb00784b34!OpenDocument>

NATIONAL

Law to order northern border counternarcotics strategy. The U.S. President likely will sign a bill in coming days to tighten security along the U.S. northern border after complaints that federal agencies there do not coordinate well enough. The bill (S. 3467), the Northern Border Counternarcotics Strategy Act, would require federal law enforcement agencies to produce a comprehensive, coordinated plan to combat the trade of illegal drugs across the U.S. northern border. A Democratic Senator from New York, the sponsor of the Senate bill, praised its passage by the House December 21, one day after the Senate passed it December 20. "Law enforcement in communities along the northern border can rest a little easier tonight knowing that resources they need to stop the flow of drugs should be on the way soon," the Senator said in a statement. "As I travel the state [of New York], one of the first things I hear from law enforcement is how they're stretched thin trying to fight the drug trade. This bill will ensure that federal law enforcement officials are working hand in glove with cops on the ground to fight drug trafficking." Source: <http://www.hstoday.us/briefings/today-s-news-analysis/single-article/law-to-order-northern-border-counternarcotics-strategy/520dd506c7b751c051e33c1ac99a94fd.html>

(California) Homes evacuated as biggest storm yet heads for California. After days of relentless rain, Southern California December 22 was facing the most intense storm system yet, with hundreds of homes evacuated, roads covered with water and mud, and residents anxiously eyeing already saturated mountainsides denuded by wildfires. A rain-soaked hillside collapsed on part of a busy Interstate 10 transition road December 22 as overwhelmed drains left hubcap-deep pools of water on roadways littered with fender-bender crashes. The landslide covered three lanes of the transition to State Route 57 in the Pomona area, and the California Highway Patrol shut down part of the ramp before the morning rush hour. More than 30 people were rescued December 22 from stranded cars and homes in hillside areas of Laguna Beach and adjoining Laguna Woods. About a square mile of Laguna Beach, including the downtown area, was closed when storm runoff sent mud and up to 4 feet of rushing water over the streets. Source: <http://www.thestar.com/news/world/article/910812--homes-evacuated-as-biggest-storm-yet-heads-for-california>

(Louisiana) Scientists find massive damage from BP oil spill in Gulf of Mexico. A thick layer of oil bearing the chemical signature of the BP Deepwater Horizon blow-out has been discovered covering thousands of square miles of sea floor in the Gulf of Mexico, according to a federal report released December 21. On a recent research vessel expedition, scientists from the National Oceanic and

UNCLASSIFIED

UNCLASSIFIED

Atmospheric Administration and the University of South Florida found high levels of toxins in a deadly blanket of oil on the sea floor measuring several centimeters thick. Scientists said all the micro-organisms and worms in the sediment were dead. Using tests called biomarkers, a University of South Florida oceanographer traced the damage to the BP oil spill. The oceanographer told the Wall Street Journal, "The chemical signatures are identical." Whistleblowers from the Environmental Protection Agency warned about the dangers of BP's extensive use of the chemical dispersant Corexit. Their reports claimed that sinking the spilled oil was more deadly than removing it from the surface.

Source: <http://www.examiner.com/political-spin-in-national/scientists-find-massive-damage-from-bp-oil-spill-gulf-of-mexico>

INTERNATIONAL

Blasts at 2 embassies in Rome; 2 hurt. Rome's police chief says all embassies have been informed about a pair of package bombs that exploded at the Swiss and Chilean embassies, injuring two people who opened them. The police chief spoke to reporters as he arrived December 23 at the Chilean embassy, where witnesses say an explosion was heard shortly after 3 p.m. One person was injured. Three hours earlier, a package bomb exploded inside an office in the Swiss Embassy, wounding the staffer who opened it. He was taken to the hospital with serious hand injuries but his life is not in danger, the Swiss ambassador said. The police chief also said a suspicious package found at the Ukrainian embassy turned out to be a false alarm. The Italian Foreign Minister condemned what he called a "deplorable act of violence," and offered Italy's solidarity with the embassy staff and the victim. There have been growing concerns in Europe about holiday season attacks following a suicide bombing in Sweden and security services' fears of an assault on a European city modeled on the deadly shooting spree in Mumbai, India. Source: http://www.usatoday.com/news/world/2010-12-23-embassy-blast_N.htm

Nigeria shuts refineries after pipeline attacks. Nigeria's state-oil company said on December 22 three of the country's four refineries were not operating because pipelines feeding the facilities were damaged in militant sabotage attacks. The Nigerian National Petroleum Corporation (NNPC) said vandalism of pipelines led it to shut down the Warri, Kaduna, and Port Harcourt refineries but it did not say how long they had been out of action. Africa's most populous nation usually imports around 85 percent of its fuel needs but purchases from foreign suppliers may increase as the refinery closures are likely to cut out most of the country's 445,000 barrel per day (bpd) refining capacity. "The rate of the crude pipeline vandalism from Bonny to Port Harcourt refinery and the Escravos to Warri and Kaduna refinery is alarming and I wish to request the army to concentrate on these pipelines as they are critical to our operations," a spokesman said. The choking off of Nigeria's local oil product supply adds to signs that a resurgence in violence by militants in the oil-producing Niger Delta region is having a significant impact on Africa's largest oil and gas industry. U.S. energy firm Chevron said this week it had suspended production from a major pipeline after a sabotage attack, while fellow oil majors Shell and Exxon have also suffered outages recently. Source: <http://www.reuters.com/article/idUSLDE6BL18720101222>

Somali pirates hijack ship using guns, grenades. Somali pirates hijacked a cargo vessel December 20 after firing rocket propelled grenades and small arms at the ship, the European Union Naval Force said. The pirates seized the MV Orna about 400 miles northeast of the island nation of the Seychelles, said a wing commander. The ship was not registered with maritime authorities so the number and

UNCLASSIFIED

UNCLASSIFIED

nationalities of crew are not known. The commander said at least four pirates boarded the vessel and the crew are cooperating and have not reported any damage. The MV Orna is a Panama-flagged, bulk cargo vessel owned by a company in the United Arab Emirates. Before the hijacking of the MV Orna, pirates were holding 23 ships and 555 hostages, according to the EU Naval Force. Source:

http://news.yahoo.com/s/ap/20101220/ap_on_re_af/piracy

Weather chaos continues to hit UK airports. Snow and freezing temperatures continued to ground flights to and from Britain December 21, with travelers hoping to get away for Christmas likely to suffer delays and cancellations for several more days. British Airways (BA) said it expects to make a “significant number of cancellations” to its shorthaul services from London’s Heathrow airport, which will again operate with just one of its two runways December 21. Thousands of passengers have been stranded at Heathrow, the world’s busiest international airport, for days as flights have been delayed and canceled. Arctic conditions have caused major disruption to operations since December 17, with BA expecting the travel chaos to continue. The British government said it had relaxed regulations on night flights at Heathrow December 20, allowing for arrivals until 1 a.m. each day until Christmas.

Source: <http://www.reuters.com/article/idUSLNE6BK01S20101221>

Bomb damages Spanish bank’s branch in Argentine capital. A bomb damaged ATMs and shattered windows December 20 at a branch of BBVA-Banco Frances, a unit of Spanish banking giant BBVA, in Buenos Aires, Argentina but no one was injured, Argentine police said. They said this was the seventh attack of this type this year. The bomb dispersed anarchist pamphlets at the bank branch in the Recoleta district about 220 yards from the French and Brazilian embassies. The pamphlets criticized repression against the Qom Indians in Formosa, a province in northern Argentina, and the death of a young man during a protest a few months ago in the southern province of Rio Negro, police said. The pamphlets also referred to the leftist Movimiento Todos por la Patria, a group whose January 1989 attack on an army base outside Buenos Aires left 39 police, soldiers and assailants dead. The bombing is being investigated by a federal judge in Buenos Aires, police said. Previous attacks, all committed in the early morning hours and resulting in no injuries, targeted Santander Rio, a unit of Spanish bank Grupo Santander, U.S.-based Citibank and state-owned Banco de la Nacion Argentina, the country’s largest bank. The judge investigating the bombings is focusing on Chilean anarchist group Celulas Revolucionarias Brigada Andrea Salsedo. The Chilean anarchist group claimed responsibility for the bombing in July of the BBVA-Banco Frances branch in Flores, a neighborhood in the western part of the capital. Source: <http://latino.foxnews.com/latino/news/2010/12/20/bomb-damages-spanish-banks-branch-argentine-capital/>

Oil pipeline explosion kills 28 in Mexico. At least 28 people were killed and 52 injured after an oil pipeline exploded in central Mexico. The cause of the December 19 explosion in San Martin Texmelucan, was under investigation, but preliminary reports pointed to the illegal extraction of oil from the pipe, said the coordinator for civil protection in Puebla. The situation is under control, but the extent of the damage was still being assessed, a Civil Protection Director said. The pipe belongs to Pemex, the state-owned oil monopoly. Some 32 houses were lost in the blast. Pemex said in a statement December 19 that 115 homes were damaged by the explosion. Video from the scene showed a huge billowing wall of smoke that reached into the sky. Thirteen of the people killed were children, the state news agency Notimex reported, citing the civil protection coordinator. About 5,000 nearby residents were evacuated, officials said, and some 200 were in a government shelter. Oil theft has been a persistent problem for Pemex, and has been on the rise since the President of

UNCLASSIFIED

Mexico took office. Source:

<http://edition.cnn.com/2010/WORLD/americas/12/20/mexico.pipeline.explosion/>

BANKING AND FINANCE INDUSTRY

New phishing campaign targets Netflix users. Security researchers from Trend Micro warn of a phishing campaign targeting Netflix customers, which produces e-mails claiming their accounts were suspended. The rogue e-mails cite credit card problems and instruct users to log into their accounts via the included link to update their payment information. The messages are titled "Your Account Has Been Suspended" and read "We are sending this email to let you know that your credit card has been expired. To update your account information, please visit Your Account." Phishers used a real Netflix e-mail template when creating the campaign in order to add credibility. It bears the company's logo, disclaimer, contact information and color scheme. The phishing attack works in two steps. The first one is meant to steal Netflix account credentials, the advertised link taking users to a Web site mimicking the Netflix log-in page. Once victims input credentials, they are redirected to a second page displaying a form to input credit card details and other financial data. Source:

<http://news.softpedia.com/news/New-Phishing-Campaign-Targets-Netflix-Users-173884.shtml>

Zeus botnet targets holiday shoppers. As holiday shoppers take advantage of the convenience of online shopping, a Zeus botnet is targeting credit-card account holders who shop several major U.S. retailers including Macys and Nordstrom. Researchers with security firm Trusteer captured and analyzed malware samples designed to steal credit card information, probably to conduct card-not-present (CNP) fraud, an analyst said in a blog post. The attack is using a Zeus 2.1.0.8 botnet, the latest and most sophisticated version of the Zeus malware platform, the analyst said. CNP fraud takes place when a credit card is not physically present at the point of sale, as in an Internet, mail, or phone purchase. In this particular attack, social engineering is used after an infected user logs onto one of the targeted retailer's card services Web site and the botnet causes a man-in-the-middle-style pop up that says: "In order to provide you with extra security, we occasionally need to ask for additional information when you access your account online. Please enter the information below to continue." In the pop-up window, the user is asked to enter several pieces of sensitive data, such as Social Security number and mother's maiden name. Source: <http://www.pcworld.com/article/214187/>

Bank of America bans WikiLeaks-related transactions. Bank of America has joined the list of companies who refuse to do business with WikiLeaks, a decision that might attract the anger of hackers. The ostracizing of WikiLeaks by financial companies as a result of "Cablegate," started in early December when PayPal, closed the organization's donations account. PayPal cited terms of service violations as a result of "activities that encourage, promote, facilitate or instruct others to engage in illegal activity." PayPal's decision was soon followed by MasterCard and Visa, who announced blocking all credit-card-based donations to WikiLeaks for similar reasons. Bank of America, the largest bank in the United States, said WikiLeaks was inconsistent with its own rules. According to the BBC, the company announced it will block "transactions of any type that we have reason to believe are intended for Wikileaks," because the organization "may be engaged in activities that are inconsistent with our internal policies for processing payments." Following the announcement, WikiLeaks and Anonymous, the group of hackers who pledged allegiance to the whistleblower site, advised people to close their Bank of America accounts. Source:

<http://news.softpedia.com/news/Bank-of-America-Bans-WikiLeaks-Related-Transactions-173696.shtml>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

EPA and European Chemicals Agency sign agreement to enhance chemical safety. The U.S. Environmental Protection Agency (EPA) and the European Chemicals Agency (ECHA) have announced a partnership to promote enhanced technical cooperation on chemical management activities. The partnership is part of EPA's commitment to improve chemical safety. ECHA is the agency that implements the European Union's chemical management program known as REACH (Registration, Evaluation, Authorization, and Restriction of Chemicals). The statement of intent puts in place a process for working together on a range of issues including, toxicity testing, hazard and risk assessment of chemicals, risk management tools, scientific collaboration, and data exchange. One of the major areas of collaboration will be on the exchange of information. For example, the statement of intent will promote the exchange of non-confidential information on hazards, uses, and substance identification between ECHA and EPA, including data collected under REACH. The two agencies will also share criteria for managing confidential business data with the goal to increase the availability of chemical information to the public. The statement also enables the agencies to share information on approaches to more efficiently address chemicals of concern prioritized for regulatory action. Source: <http://yosemite.epa.gov/opa/admpress.nsf/0/39E0AC05307F270A852577FC0068C184>

COMMERCIAL FACILITIES

Holiday season prompts stepped-up security against terrorist attack. National-security officials and law-enforcement agencies have stepped up efforts to prevent a terrorist attack in the United States during the holiday season. "We are concerned these terrorists may seek to exploit the likely significant psychological impact of an attack targeting mass gatherings in large metropolitan areas during the 2010 holiday season, which has symbolic importance to many in the United States," warns a recent bulletin sent to law-enforcement agencies by the Federal Bureau of Investigation and the Department of Homeland Security. Of particular concern are public gatherings such as sporting events, parades, and religious or cultural activities. "Attacks against air cargo during this busy season are also a concern," states the bulletin. At a White House briefing December 22, the chief counterterrorism adviser to the U.S. President outlined steps taken since last year. Officials base their concern this holiday season on "increased chatter" among individuals and organizations associated with terrorism. "There is a lot of chatter in the intel world ... that references the holidays," the Secretary of Homeland Security told ABC on December 20. "We know that things have already happened in Europe, and we're watching that very closely as well." Source: <http://www.csmonitor.com/USA/2010/1222/Holiday-season-prompts-stepped-up-security-against-terrorist-attack>

(New York) Suspicious package shuts down Macy's. A suspicious package caused the evacuation of Macy's department store in the middle of the holiday shopping rush December 20 in New York City. Police closed off Broadway from 34th to 35th Streets and Herald Square in New York after a call came in at about 12:30 p.m. concerning a suspicious suitcase in front of the store, police said. Shoppers and employees were evacuated from Macy's as the bomb squad inspected the package, police on the scene said. Police reopened the store and gave the all clear at 2 p.m. after a member of the counter

UNCLASSIFIED

terrorism unit, clad in a bomb suit, cut open the suitcase and found clothing inside. Source: <http://www.dnainfo.com/20101220/midtown/suspicious-package-shuts-down-macys>

(California) Choir 'flash mob' forces evacuation of Roseville Galleria. The Westfield Galleria in Roseville, California, was evacuated December 20 after fears of overcrowding. Several thousand people gathered in the food court on the second story of the mall for a performance organized by the Sacramento Choral Society, according to a Roseville Fire Department spokesman. He said the first 911 call came at 6:30 p.m. Somebody reported hearing two pops that sounded like the floor was giving way, and another person said the floor was shifting. Between 40 and 50 calls then flooded 911, all of the callers worried about the floor starting to shift or too many people gathered in one spot in the mall. Emergency personnel began arriving at 6:45 p.m. and immediately started evacuations. Two engineers from the Roseville building department were inspecting the floors to test their structural integrity. The California Highway Patrol's (CHP) Traffic Management Center reported the CHP closed the exits from Highway 65 to Galleria Boulevard to prevent more traffic from entering the area. Galleria shoppers reported officials announced the evacuation over the public address system shortly after 7 p.m. Witnesses reported that crowds were calm and there was no sign of panic. Source: <http://www.modbee.com/2010/12/20/1480437/roseville-galleria-evacuation.html>

(Louisiana) Police deactivate 'device'. Fifty houses and three apartment buildings were evacuated December 18 while officials took steps to make sure a suspicious device found near the Islamic Center of Lafayette in Louisiana was deactivated safely. "State police emergency service personnel were able to render the device safe," said a Louisiana State Police spokesman. He said a telephone tip led police to a briefcase leaning against a fence near the Islamic Center. Although he did not say what was in the briefcase, he did say the device was a threat that required special care and precautions. Representatives of the FBI, Lafayette Fire Department, Lafayette Police Department, state police, and their respective hazardous materials teams responded. Officials cordoned off nine city blocks encompassing West University Avenue and St. Mary Boulevard, and Taft and Harding streets. A Lafayette police spokesman said people were inside the Islamic Center at the time of the call. The spokesman said they could not rule out explosive or chemical agents in the briefcase. The suspicious package at the Islamic Center comes on the heels of a car that was set on fire at the center September 21. Source: <http://www.theadvertiser.com/article/20101219/NEWS01/12190327/1002/Police-deactivate--device->

COMMUNICATIONS SECTOR

Divided FCC adopts rules to protect Web traffic. Federal regulators adopted new rules December 21 to keep the companies that control the Internet's pipelines from restricting what their customers do online or blocking competing services, including online calling applications and Web video. The new rules have the backing of the White House and capped a year of efforts by the FCC Chairman to find a compromise. They are intended to ensure that broadband providers cannot use their control of the Internet's on-ramps to dictate where their subscribers can go. They will prohibit phone and cable companies from favoring or discriminating against Internet content and services that travel over their networks — including online calling services such as Skype, Internet video services such as Netflix, and other applications that compete with their core businesses. The prohibitions, known as "net neutrality," have been at the center of a Washington policy dispute for at least five years. Source:

UNCLASSIFIED

<http://www.google.com/hostednews/ap/article/ALeqM5gyoWGBFkAi1iWOw16boaHXwpf0kg?docId=30e116bd6db54942b7bca7fa8b0b9e11>

Google DNS slowing down iTunes and Apple TV. AppleInsider reported December 22 on a potential cause for slow Apple TV and iTunes download speeds: the use of Google's DNS servers. Last year Google started a public DNS service, promising faster speeds and security, but AppleInsider mentions that because some download services use the DNS server to locate the nearest download server, using Google's DNS servers (which are at one location) will route everyone to the download server closest to them and bog it down. Source: http://reviews.cnet.com/8301-13727_7-20026241-263.html

(Hawaii) Bomb squad removes improvised device from Waipahu Civic Center. An unknown person tried to set off an improvised explosive device December 16 at the Waipahu Civic Center in Hawaii, police said. Personnel from the center called police about 7 a.m. after finding a plastic Pine-Sol bottle partially filled with a dark gray, powdery substance, and a partially burned hand towel underneath, police said. A bomb squad from the specialized services division was called in and removed the bottle. No one was injured and there were no damages. Source: <http://www.staradvertiser.com/news/breaking/112118729.html>

BitTorrent domain exodus continues as Torrentz dumps .com. The Internet's second biggest BitTorrent site is dumping its .COM domain. In an apparent response to the U.S. Government's Department of Homeland Security and Immigration and Customs Enforcement recent seizures of domain names, the site moved to a new home. Despite being only a meta-search engine, Torrentz.com appears to be taking no chances with an immediate .EU domain migration. The fallout from the November domain name seizures carried out by U.S. authorities continues to spread in the file-sharing community. Torrent-Finder, which shifted to a .INFO domain to continue its operations, is fighting back with legal representation. Others, unsettled by the developing atmosphere of uncertainty, are taking steps to mitigate potential future action against their sites. Already several private trackers have invested in alternative domain names that are at least currently believed to be outside U.S. control or influence. The popular Demonoid tracker showed its hand with a shift from a .COM to a .ME domain. Source: <http://torrentfreak.com/bittorrent-domain-exodus-continues-as-torrentz-dumps-com-101218/>

CRITICAL MANUFACTURING

Govt upgrades investigation of Ford minivans. The U.S. government has upgraded its investigation into Ford Windstar minivans amid additional concerns over corrosion in the vehicles. The National Highway Traffic Safety Administration (NHTSA) says in a posting on its website December 22 that it has begun an engineering analysis of about 550,000 Windstars from the 1999-2003 model years. Ford has recalled more than 600,000 of the minivans in the U.S. and Canada since August 2010 to address rear axles that can corrode and break. The U.S. recall is limited to 22 cold weather states where road salt is used during the winter. The government says it has received 346 complaints of corrosion and breaking of the front subframe, which carries the engine, transaxle, steering rack, and front suspension. NHTSA says it is trying to learn more about the alleged defect. Source: <http://www.businessweek.com/ap/financialnews/D9K91T000.htm>

UNCLASSIFIED

Toyota paying \$32.4 million fine for sticky pedals. Toyota has agreed to pay the U.S. government an additional fine of \$32.4 million for failure to alert U.S. authorities about defects like sticky gas pedal and steering, which led to massive recall of cars around the world. Toyota in April had earlier been fined \$16.4 million by the National Highway Traffic Safety Administration (NHTSA). The total fine imposed on the company because of the recalls, will be nearly \$50 million, reports the Associated Press. The decision to pay the penalty was taken by Toyota to avoid further litigation with U.S. authorities. The company still claimed it did not conceal the problem from consumers and the U.S. government. According U.S. Department of Transportation representatives, the agreement to pay fines does not relieve the Japanese company from lawsuits brought against it by its clients. Toyota will have to pay compensation to all owners of cars the court deems injured due to the fault in the cars. From late 2009 to early 2010, Toyota and Lexus withdrew more than 8.5 million cars worldwide, 5 million of which were found to have sticky gas pedal. A service campaign for 1 million cars was carried out to eliminate potential steering problems. Source: <http://seerpress.com/toyota-paying-32-4-million-fine-for-sticky-pedals/18933/>

Car immobilizers easily circumvented by crafty carjackers. Weak cryptography means car engine immobilizer technology has become easy for crooks to circumvent. Nothing weaker than 128-bit AES is considered sufficient protection for e-commerce transactions, but car manufacturers are still using proprietary 40-bit and 48-bit encryptions protocols that are vulnerable to brute force attacks. Worse still, one unnamed manufacturer used the Vehicle Identification Number (VIN) as the “secret” key for the immobilizer. The weakness of the technology was recently exposed in security research by an ethical hacker from Security Research Labs, who links the weakness with a growth in car thefts in Germany in 2009, following years in decline. Source: http://www.theregister.co.uk/2010/12/20/car_immobiliser_security_flaws/

DEFENSE/ INDUSTRY BASE SECTOR

Study flags risks to US missile defense program. The U.S. President’s planned missile defense system for Europe could prove unreliable and risks delays and cost over-runs, congressional investigators said in a new report. The United States announced plans in 2009 to integrate sea- and land-based missile defenses in Europe, a program referred to as the “European Phased Adaptive Approach.” U.S. anti-ballistic missile systems are meant to cover Europe by around 2018, and NATO allies in Europe agreed in November to bolster the missile shield. But the Government Accountability Office warned in a report dated December 21 that there was limited visibility into the costs and timetable for the program. It warned that one of the consequences could be “going into production before fully demonstrating system performance, leading to rework, cost increases, delays, and uncertainties about delivered capabilities.” The United States has already spent more than \$10 billion a year on a range of missile defense programs in recent years, but critics say those programs are still far from reliable. Source: <http://in.reuters.com/article/idINIndia-53740620101222>

Bergen defense contractor admits selling knockoff parts for U.S. military vehicles. The majority owner of a Bergen, New Jersey-based defense contractor admitted December 17 his firm sold the government used brake drums and other parts it passed off as new for use in military operations. The Turkish national, from Teaneck, entered a guilty plea in federal court in Newark on behalf of New York Machinery (NYM). Overall, the broken contracts cost the Department of Defense (DOD) \$163,082 in losses, which will be repaid under the plea agreement, a spokesman for the U.S. Attorney

UNCLASSIFIED

said. The DOD contracts were to provide replacement parts for use in military tow tractor-trailers. Under a contract that ran through March 2005, the parts were to be “exact products” manufactured by or under the direction of an original equipment manufacturer, said a spokesman from the U.S. Attorney’s office. NYM substituted knockoffs manufactured in Turkey and re-labeled them to look like the genuine “made in the USA” article, according to a team of federal prosecutors. The company knew the specs of the items after another operation owned by the defendant bought genuine parts from the United States that were manufactured in Turkey, the team said. NYM then simply “reverse-engineered” copies of the original equipment manufacturer parts, they said. Source: <http://www.cliffviewpilot.com/beyond/1929-turkish-defense-contractor-admits-selling-knockoff-parts-for-us-military-vehicles>

EMERGENCY SERVICES

ATF seeks emergency authority to crack down on gun smugglers. The Bureau of Alcohol, Tobacco, Firearms (ATF) is asking the White House for emergency authority to try to crack down on gun smugglers. The ATF wants the power to require dealers near the Mexican border to report multiple purchases of high-powered rifles. The new policy would affect customers who buy two or more guns in a 5-day period from the same dealer. The move is intended to help Mexican authorities fight the cartels. The ATF is asking the White House to sign off on its request by January 5. Source: http://www.krgv.com/news/local/story/ATF-Seeks-Emergency-Authority-to-Crack-Down-on/0wpwG_gFx0qMH_mipIQlvG.cspX

(Florida) Coast Guard investigates hoax distress calls. The U.S. Coast Guard is investigating a series of hoax mayday calls made in November near Hobe Sound, Florida. Coast Guard officials said December 20 the hoax distress calls were made in early November from a person in the vicinity of Hobe Sound. When asked to provide his position, the caller provided false GPS coordinates. In one of the distress calls, the caller claimed the hull of his boat was cracked. The calls were made on a radio channel reserved for emergency communication. Coast Guard officials said they triangulated a general area where the calls originated. Under federal law, knowingly and willfully transmitting a hoax distress call is a felony punishable by up to 6 years in prison, a \$250,000 fine, and restitution to the Coast Guard for all costs incurred while responding to the call. Source: <http://www.wpbfl.com/r/26197295/detail.html>

(Georgia) 700K Ecstasy tabs seized, Customs agent arrested. Prosecutors in Georgia said they have seized 700,000 tabs of Ecstasy and have charged a U.S. Customs and Border Protection agent and 13 others in what they say was a large-scale, drug trafficking scheme. A U.S. Attorney said December 16 authorities seized the Ecstasy worth more than \$2.8 million at a house in Chamblee in northeast Atlanta. The Customs agent is charged with laundering drug money, smuggling cash, and attempting to bring weapons onto an aircraft. Prosecutors said an officer posing as a money launderer gave the 45-year-old man \$22,000, which they said he smuggled to Jamaica. He is also charged with conspiracy to commit marriage fraud. Authorities said he was paid \$900 to help a couple in a sham marriage deceive Customs officials. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/16/AR2010121604821.html>

More sex-offender alerts sent via e-mail. A growing number of law enforcement agencies and states are using e-mail to alert victims and anyone else who wants to know when sex offenders in their area

UNCLASSIFIED

move into the neighborhood, or change jobs or schools. The Missouri State Highway Patrol and the Sacramento, California police and sheriff's departments are among the latest agencies to unveil such systems, adding them in October and November respectively. Statewide systems are in place in a dozen states, including Alabama, Florida, Louisiana, Ohio, and South Carolina, said the vice president of sales and marketing for Watch Systems of Covington, Louisiana, which has partnered with several states to develop their systems. Indiana and Illinois are in the process of implementing systems that will give them similar capabilities along with other technology to track sex offenders, he said. The system allows anyone to enter an address and get e-mails when a sex offender registers a home, work or school address near them, he said. Source: http://www.usatoday.com/news/nation/2010-12-17-sexoffenderalerts17_ST_N.htm

Cameron County deputy admits to firearms smuggling. A Cameron County Sheriff's Deputy in Brownsville, Texas has admitted to attempting to permit a load of semi-automatic firearms to be unlawfully exported into Mexico in exchange for money, a U.S. Attorney announced December 17. The 31-year-old man, of Brownsville, has been a Cameron County sheriff's deputy since March 2006. He pleaded guilty to the federal felony charge — admitting that on May 5, 2010, while assigned to the Veterans' and Gateway Ports of Entry to prevent stolen vehicles from leaving the United States, he attempted to send and export 13 semi-automatic firearms into Mexico. According to court records, he contacted the driver of a vehicle containing 13 semi-automatic weapons via cellular telephone to instruct him when he could cross into Mexico without inspection by state and federal authorities. The driver was actually an undercover federal agent. The guard admitted he knew the vehicle contained firearms and the driver did not have a license to export firearms. He believed the firearms were unlawful for export and were intended for use by a Mexican drug cartel. He accepted payment of \$4,000. Source: <http://www.kztv10.com/news/cameron-county-deputy-admits-to-firearms-smuggling/>

ENERGY

Feds want coal mines to expand scope of exams. Federal regulators December 22 sought to require coal operators to inspect their underground mines for health and safety violations, in addition to the hazard checks they now conduct. The U.S. Mine Safety and Health Administration (MSHA) proposed revised rules governing the exams that operators must perform before and during work shifts, as well as weekly and as follow-ups. "Examinations are the first line of defense for miners working in underground coal mines," the MSHA director said. "Mine operators must take ownership for their workers' health and safety by conducting basic workplace examinations to ensure they are in compliance with health and safety standards." The current regulations require that operators identify, correct, and record hazardous conditions during these exams. In seeking to expand that to cover violations of mandatory health or safety standards, MSHA cited its review of accident investigation reports and its own enforcement actions going back five years. The proposed rule change would also require operators to review all citations and enforcement orders with regulators every three months. The agency said that its inspectors issued 82,126 citations and orders at underground coal mines last year. Source: <http://www.dailymail.com/ap/ApTopStories/201012221120>

DOT releases pipeline guidelines to assist communities. The U.S. Department of Transportation (DOT) released new guidelines December 16 to help local governments, developers, and community

UNCLASSIFIED

UNCLASSIFIED

planners do a better job of protecting areas near pipelines. The guidelines, which the Pipelines and Informed Planning Alliance developed, marked the first time recommendations for development near existing transmission pipelines have been issued, DOT said. It said the report, "Partnering to Further Enhance Pipeline Safety Through Risk-Informed Land Use Planning," offers nearly 50 recommended practices for communities, developers, and pipeline operators to use to reduce safety risks resulting from community growth near pipelines. DOT said the suggestions explain how land use planning and development decisions can help protect existing pipelines. They also provide recommendations on how communities can gather information about local pipelines; about how local planners, developers, and pipeline operators should communicate during all development phases; and how to minimize pipeline damage from excavation during site preparation and construction. Source:

http://www.pennenergy.com/index/petroleum/display/9459914393/articles/oil-gas-journal/transportation-2/pipelines/2010/12/dot-releases_pipeline.html

(Washington) Storm cuts power to 112,000; rural home burns. A windstorm blew through Washington December 17 and December 18, toppling trees and power lines with gusts reaching 70 miles per hour. At its height, the storm knocked out electricity to an estimated 112,000 utility customers in King, Pierce, and Snohomish counties. Outages were heaviest in South King County, where crews had to back off tending to downed lines December 18 because of high winds. About 27,000 Puget Sound Energy (PSE) customers were without power early December 18, mostly around the Enumclaw, Cumberland, and Maple Valley area, a PSE spokeswoman said. PSE had 130 people in the field working to restore power, along with 45 others from elsewhere in Washington and Oregon. In Seattle, about 12,000 Seattle City Light customers were without power early December 18, primarily in the Magnolia, Queen Anne, and south Beacon Hill neighborhoods, and in parts of the Fremont neighborhood. By December 18, power was restored to all but 400 customers, the utility said. Source: http://seattletimes.nwsources.com/html/localnews/2013713981_weather19m.html

FOOD AND AGRICULTURE

Food safety bill approved by Congress. A food safety bill (H.R. 2751) has been approved by both the U.S. House of Representatives and Senate. The President has announced that he will sign the bill. Under the measure, companies that manufacture, process, pack, distribute, receive, hold, or import food would be required to implement safety measures to protect that food from contamination. Companies would be required to test these measures on an ongoing basis and document the outcomes. The government would establish regulations to prevent the intentional adulteration of food. Source: <http://www.securitymanagement.com/print/8019>

Texas firm recalls ground beef products. Winn Meats Co., a Dallas, Texas, establishment, is recalling approximately 25,600 pounds of ground beef products that were improperly labeled and potentially adulterated, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced December 20. The products' labels include "For Cooking Only," indicating that they are intended for further processing to apply a full lethality at a federally inspected establishment. Because the products were distributed to non-federally inspected establishments where it cannot be verified that sufficient further processing occurred to remove foodborne pathogens that could have been present, these products must be removed from commerce. The following products are subject to recall: "60-pound boxes of 'Ground Beef for Cooking Only.'" Each box bears the establishment number "EST. 2338" inside the U.S. Department of Agriculture mark of inspection and can be

UNCLASSIFIED

UNCLASSIFIED

identified by the case code “506093.” Boxes contain three 20-pound packages of ground beef. The ground beef products were produced between August 24, 2010 and November 30, 2010. They were sent to a distribution center in Albuquerque, New Mexico, who in turn sent the products to restaurants, central kitchens, and caterers throughout the state. Source:

<http://www.myhealthnewsdaily.com/texas-firm-recalls-ground-beef-products-0923/>

Scientific American: U.S. pig farms may be ‘flu factories’. The H1N1 in pandemic in 2009 was a wake-up call to many scientists to how unpredictable and dangerous viruses circulating in the animal world can be if they jump to humans. Since then, there has been a lot of talk about monitoring the health of the animals most likely to pass on a flu virus with pandemic potential — pigs and birds. An article just published in Scientific American says pig monitoring in the United States is very poor. Monitoring is so bad that American pigs farms are virtually “flu factories,” according to the author of the report. The problem, he writes, is that the pork industry is reluctant to share data with human health officials, and that industry results of pig flu tests are kept confidential. Source:

<http://www.npr.org/blogs/health/2010/12/23/132256243/scientific-american-u-s-pig-farms-may-be-flu-factories>

Pet food recall: Is your pet’s food on the list? The Kroger Co. announced December 18 it was recalling three brands of pet food sold in stores in 19 states. Tests showed select packages may have come into contact with aflatoxin, which can kill or seriously injure pets. Customers who bought contaminated feed should stop using it immediately and return it to the place of purchase for a refund or exchange. The affected packages of Pet Pride, Old Yeller, and Kroger Value brand pet foods were produced at a Kroger-owned factory in Springfield, Tennessee, said a spokeswoman for the Cincinnati-based grocery store. The recall affects customers at Kroger’s, Dillons, Gerbes, Baker’s, Food 4 Less, Jay C, Hilander, Owen’s, Pay Less and Scott’s stores in 19 states, including: Alabama, Arkansas, Georgia, Illinois, Indiana, Kansas, Kentucky, Louisiana, Michigan, Mississippi, Missouri, Nebraska, North Carolina, Ohio, South Carolina, Tennessee, Texas, Virginia, and West Virginia. The products have a sell-by date of October 23 or 24, 2011. The package reads: OCT 23 11 DP or OCT 24 11 DP. The recalled products are: Pet Pride Cat Food sold in 3.5 lb. and 50 lb. packages. Pet Pride Tasty Blend Poultry & Seafood Cat Food sold in 3.5 lb. and 18 lb. packages. Pet Pride Kitten Formula Food sold in 3.5 lb. packages. Old Yeller Chunk Dog Food sold in 22 lb. and 50 lb. packages. Kroger Value Cat Food sold in 3 lb. packages. And Kroger Value Chunk Dog Food sold in 15 lb. and 50 lb. packages. Customers who have questions about this recall may contact Kroger toll-free at (800) 632-6900 or visit the recalls tab on Kroger’s Web site. Source: <http://www.csmonitor.com/Business/new-economy/2010/1221/Pet-food-recall-Is-your-pet-s-food-on-the-list>

Food safety bill unexpectedly passes Senate. A bill that would overhaul the nation’s food-safety laws for the first time since the Great Depression came roaring back to life December 19 as Senate Democrats struck a deal with Republicans that helped overcome a technical mistake made 3 weeks ago and a filibuster threat that seemed likely to scuttle the legislation. After a weekend of negotiations, tense strategy sessions and several premature predictions about the bill’s demise, the Senate majority leader, a Democrat, reached a deal with the minority leader, a Republican, that the GOP would not filibuster. Without notice and in a matter of minutes that evening, the Senate approved the bill by unanimous consent, sending it to the House, where passage is expected. The U.S. President has said he would sign the legislation, which would give the government far-reaching authority to set and enforce safety standards for farmers and food processors. The legislation would

UNCLASSIFIED

UNCLASSIFIED

affect all whole and processed foods except meat, poultry and some egg products, which are regulated by the U.S. Department of Agriculture. Source:

<http://www.dailymail.com/News/201012201687>

Al Qaeda group contemplated poisoning food in U.S., officials say. The al Qaeda group that built two toner-cartridge bombs in an unsuccessful attempt to blow up planes in October also has contemplated spreading poison on salad bars and buffets at U.S. hotels and restaurants, U.S. officials told CNN December 21. But U.S. officials sought to downplay the threat — first reported by CBS News — saying it was months old, and that it was more in the nature of a discussion of “tactics” than an actual plot. Officials implied the tactic is beyond the capabilities of the terrorist organization, which is based in the Middle East. The United States has received information that al Qaeda was considering the tactic of placing ricin and cyanide poisons into food supplies, DHS officials confirmed to CNN. In response to that information, U.S. officials met through regular channels with representatives of the hotel and restaurant businesses to discuss the possibility that terrorists could target the food supply, and to reiterate “best practices” to ensure the food supply is safe. Officials, however, likened the threat to numerous others discussed in jihadist publications such as the online magazine Inspire, where al Qaeda members and sympathizers discuss various ways to attack Western countries. “We’re talking months, not weeks (ago), that this came into the threat stream,” one official said. Another U.S. official said, “We’re aware that terrorists have been interested in doing this kind of thing for a long time. They’ve said as much and, as a result, we take all of this very seriously. But we don’t know of any current plotting along these lines.” Source:

<http://edition.cnn.com/2010/US/12/21/al.qaeda.poison.plot/>

(Texas; New Mexico) Texas firm recalls mislabeled ground beef. Winn Meats Co of Dallas, Texas, is recalling approximately 25,600 pounds of ground beef products that were improperly labeled and potentially adulterated, the U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) announced December 17. The products’ labels include “For Cooking Only,” indicating they are intended for further processing to apply a full lethality at a federally inspected establishment. But because the products were distributed to non-federally inspected establishments, whether sufficient processing occurred to remove potential pathogens cannot be verified, so the products must be removed from commerce, FSIS said. Each 60-pound box of “Ground Beef for Cooking Only” bears the establishment number “EST. 2338” inside the USDA mark of inspection and can be identified by the case code “506093.” Boxes contain three 20-pound packages of ground beef. The ground beef products were produced between August 24, 2010 and November 30, 2010. They were sent to a distribution center in Albuquerque, New Mexico, which in turn sent the products to restaurants, central kitchens, and caterers throughout the state. Source:

<http://www.foodsafetynews.com/2010/12/texas-firm-recalls-mislabeled-ground-beef/>

E. coli prompts recall of gourmet raw milk cheese. A Pacific Northwest cheesemaker has been linked through an epidemiological investigation to an E. coli outbreak, resulting in a nationwide recall of all its gourmet raw milk cheese and revealing sanitation problems at the dairy. The U.S. Food and Drug Administration announced December 17 that Sally Jackson Cheese of Oroville, Washington, had agreed to recall its cheese after eight people were stricken with an identical strain of E. coli O157:H7. The eight are residents of Oregon, Washington, Vermont, and Minnesota. Onset of their illnesses ranged from September into November. One person required hospitalization. Source:

<http://www.foodsafetynews.com/2010/12/e-coli-prompts-recall-of-gourmet-raw-milk-cheese/>

UNCLASSIFIED

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(New York) U.N. quarters evacuated due to suspicious odor. The U.N. Security Council's quarters and the General Assembly were evacuated December 21 after officials noticed a "suspicious odor." Diplomats were moved to a separate building within the U.N. complex, located next to the East River in Manhattan, New York. The incident may have been caused by high river tides, creating problems with sewage in the area and within the U.N. facility, said the U.N. deputy spokesman. "It was very strong smelling and smelled a lot like gasoline," a CNN producer said. Authorities had been investigating the possibility of a combination of sulfur and methane, the U.S. Ambassador said after speaking with fire officials. U.N. officials later said the gases involved were not harmful, the spokesman said. Source: <http://www.cnn.com/2010/US/12/21/new.york.un.odor/?hpt=T2>

U.S. reports threat against embassy in Stockholm. The U.S. State Department said the U.S. Embassy in Stockholm, Sweden, has stepped up its security after receiving an unspecified threat. The embassy said in a notice to American citizens in Sweden December 20 that it decided to boost its security posture in light of the threat, a suicide bombing the week of December 13, and an increased threat level in the country. The notice gave no additional details but said its additional security measures were "prudent and necessary." The week of December 13, a suicide bomber killed himself and injured two people when some of the bombs he was wearing exploded among panicked Christmas shoppers in downtown Stockholm. Police suspect the explosives went off accidentally near a pedestrian street, and that the suspect planned to detonate them in a place where they would inflict more damage. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/20/AR2010122004367.html>

National Guard copter crashes off San Juan. A U.S. Army National Guard helicopter crashed in the waters off San Juan, Puerto Rico, December 20 with at least one person reported dead, media reports said. CNN, citing a Federal Aviation Administration spokeswoman, said at least one person died in the crash. Noti Uno radio in Puerto Rico broadcast all six people on board had died, but the information was not posted on its Web site. "The preliminary information we have ... is that the wreckage of (the) Army National Guard aircraft was found in the water near San Juan," a spokeswoman told CNN in an e-mail. The helicopter was destroyed. A lieutenant commander of the U.S. Coast Guard in Miami confirmed the crash occurred December 20. The Coast Guard received the call for help with search and rescue efforts, a Coast Guard spokesman in San Juan said. He said three crew members and three passengers — one guard and two civilians from Puerto Rico — were on board. The UH 72 Lakota helicopter was about 1 nautical mile northeast from the Puerto Rican coast when it crashed, officials said. Source: http://www.upi.com/Top_News/World-News/2010/12/21/National-Guard-copter-crashes-off-San-Juan/UPI-37701292944639/

Officials: CIA station chief pulled from Islamabad. The CIA has pulled its top spy out of Pakistan after terrorists threatened to kill him, current and former U.S. officials said, an unusual move for the United States and a complication on the front lines of the fight against al-Qaida. The CIA station chief was in transit December 16 after a Pakistani lawsuit earlier this month accused him of killing civilians in missile strikes. CIA airstrikes from unmanned aircraft have killed terrorist leaders, but have led to accusations in Pakistan that the strikes kill innocent people. The U.S. does not acknowledge the

UNCLASSIFIED

missile strikes, but there have been more than 100 such attacks this year — more than double the amount in 2009. Source: <http://www.google.com/hostednews/ap/article/ALeqM5j8-dDSHBIB-JIG2HZtrWzhyuhvXw?docId=81dde8ed00cb41149d173c427fc0cf63>

Jordanian held over attack on US embassy vehicle in Yemen. Yemeni police said they had arrested a Jordanian who tried to attack a U.S. Embassy vehicle in Yemen's capital. The vehicle was attacked by a hand grenade December 15 in Hadda, a Sanaa suburb, where it was parked in front of a restaurant frequented by Westerners. None of the four American Embassy personnel, who were in the vehicle, was injured. Reports quoting Yemeni security sources said police escorting the American Embassy staff arrested the young man immediately after the incident on suspicion of his involvement in the attack. Weapons and false identity papers were seized from his car, parked outside a pizza restaurant. Police are questioning the Jordanian mechanic, who resides in Yemen, to confirm if he is linked to al-Qaeda. The United States has warned its citizens in Yemen to remain vigilant about their personal security in the wake of the attack. In a travel advisory posted on its Web site December 16, the U.S. Embassy in Sanaa urged American citizens to avoid their presence in sensitive areas with a history of militant attacks. Source:

<http://www.rttnews.com/Content/GeneralNews.aspx?Node=B1&Id=1509772>

California man charged with trying to sell military jet to Iran. Federal agents have arrested a California man who allegedly attempted to export a U.S. military fighter jet to Iran, authorities announced December 17. The arrest followed a 7-month government sting operation, authorities announced. The 35-year-old also was charged in a criminal complaint with two felony counts of attempting to export other aircraft parts and controlled technology. The man has agreed to plead guilty to the charges, according to an assistant U.S. attorney, who is prosecuting the case. According to unsealed court documents, the case began to unfold after "a cooperating defendant" in the operation introduced the suspect to an undercover agent. As part of the sting, the agent met with the man on several occasions at locations in California, Pennsylvania, Delaware, and Budapest, Hungary, the court papers said. The documents said the man broached to an undercover agent the idea of obtaining an F-5B fighter jet from a source in California. He allegedly told the agent that the "Iranians" might be interested in the fighter jet and other items, and allegedly said he would not be concerned if the jet or the other items ended up in Iran. In July, the suspect allegedly sent a contract for the fighter jet to the undercover agent and demanded a \$3.25 million purchase price. He was arrested in Delaware in July while negotiating plans to fly the aircraft from California to the East Coast, where it subsequently was to be crated and shipped to Hungary and eventually Iran, the documents stated. Source: <http://edition.cnn.com/2010/CRIME/12/17/california.iran.sting/?hpt=T2>

U.S. begins evacuation of embassy staff in Cote d'Ivoire. The United States has begun evacuating dependents and non-emergency personnel from its embassy in Abidjan, the capital of Cote d'Ivoire. A U.S. State department spokesperson said December 17 the undersecretary for management approved the authorized departure of its citizens. The North America Correspondent of the News Agency of Nigeria (NAN) reported post-presidential election violence in the West African country had escalated in the previous 2 days. The Ivorian incumbent leader has refused to concede electoral defeat in spite of pressures from the international community. On December 16, the U.S. government said a rocket strike hit the outer perimeter of its embassy in Cote d'Ivoire, with only slight damage and no injuries. The outbreak of violence the same day around the capital killed more than a dozen

UNCLASSIFIED

people. Source: http://234next.com/csp/cms/sites/Next/News/Metro/Politics/5655590-146/u.s._begins_evacuation_of_embassy_staff.csp

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Facebook scams start attracting international audiences. Security researchers who analyzed recent Facebook survey scams said international users are clicking on spammed links in larger numbers than before. There are myriad scams running every day on Facebook, and many promise access to intriguing videos. The spam messages they generate usually start with “OMG” in order to make them more appealing to users. Researchers from Finnish security vendor F-Secure recently set out to investigate some of them and used Facebook’s search feature to locate posts that contained OMG and links. When they realized many scams were abusing the bit.ly URL shortening service, which happens to provide statistics for the links it generates, they decided to check how successful they really are. One scam’s links registered a number of 50,377 clicks: 18,735 from the United States, 15,825 from Sweden, and 3,481 from Belgium. Another scam registered a number of 27,400 total clicks, which had a distribution of 12,445 clicks in the United States, 8,137 in Malaysia, and 2,373 in Singapore. “This is the first time that we’ve noticed people from such countries clicking on Facebook spam in such numbers. Typically we’ve seen such tabloid style spam pulling in folks from the USA/UK, or vice versa,” the F-Secure researchers noted. Source: <http://news.softpedia.com/news/English-Facebook-Scams-Start-Attracting-International-Audiences-174310.shtml>

Fake iTunes email alerts lead users to drive-by download. A wave of fake iTunes e-mails falsely alerting recipients about their accounts facing suspension directs them to a Web page that tries to install malware on their computers. The rogue e-mails are crafted to appear as if they originate from a contact@itunes(dot)com address and bear a subject of “iTunes account may be suspended.” This sounds like a phishing scam, but the general manager of the security software division at GFI said the intention of the attackers is to silently infect users. The cyber criminals behind the e-mails even try to earn people’s trust noting in the e-mail that “iTunes will never ask you for your password or any confidential information.” Satisfied this is probably not a phishing attack, users might click on the link to see additional information. If they do, they are taken to a page mimicking an Apple support article entitled “How to report an issue with Your iTunes Store purchase.” The site might look benign, but in the background it loads scripts that try to exploit vulnerabilities in outdated versions of Flash Player, Java, and even unpatched Windows installations, to download and install malware. Source: <http://news.softpedia.com/news/Fake-iTunes-Email-Alerts-Lead-Users-to-Drive-By-Download-174137.shtml>

Database of routers’ embedded private SSL keys published. The recent publishing of a database containing over 2,000 private SSL keys hard-coded into various routers — with their corresponding public certificates and hardware/firmware versions — has made an attack that involves decrypting the traffic going through the device very easy to execute. “While most of these certificates are from DD-WRT firmware, there are also private keys from other vendors including Cisco, Linksys, D-Link, and Netgear,” said a member of the /dev/ttyS0 group that is behind this project called LittleBlackBox. “Many routers that provide an HTTPS administrative interface use default or hard-coded SSL keys that can be recovered by extracting the file system from the device’s firmware. Private keys can be recovered by supplying LittleBlackBox with the corresponding public key. If the public key is not readily available, LittleBlackBox can retrieve the public certificate from a pcap file, live traffic capture,

or by directly querying the target host,” he wrote. He offered the LittleBlackBox’s code for download. Source: <http://www.net-security.org/secworld.php?id=10348>

Worm blocks access to Facebook. A relatively new worm Symantec named “W32.Yimfoca” presents a never before seen modus operandi. A variant of the worm spreads via Yahoo! Messenger and, once installed, downloads and installs W32.Yimfoca on the target system. Lately, it has been noticed it specifically targets Facebook users by denying them access to their accounts if they do not complete a survey. Every time a user lands on the Facebook homepage, a window offering the surveys pops up. Also, while the victim fills out the survey, a progress bar is shown accompanied by a “threat” — “You have only 3 minutes to fill out the selected survey or you will not have access to your account.” Once the user has completed a survey he/she can access his/her account. If the user does not complete the survey within 3 minutes, the worm will not allow him/her to access the account while it is running — and it resets even after a reboot of the infected computer. The worm blocks access to Facebook only if Internet Explorer is being used. Using any other browser fails to trigger the worm and a user can access his/her Facebook account without being sidetracked by pop-ups. Source: http://www.net-security.org/malware_news.php?id=1575

New wave of fake Amazon emails spreads malware. Security researchers from Sophos warned a new wave of fake e-mails posing as shipment updates from Amazon are distributing an autorun worm. The rogue e-mails bear a subject of “Shipping update for your Amazon.com order” and their header is spoofed to appear as if they originate from an order-updateATamazon.com address. The contained message consists of the same text as the subject, plus an alleged order number and instructions to “check the attachment and confirm your shipping details.” In addition, the body contains an Amazon advertising banner and an image of an opened box, which were probably copied from a legit e-mail. The attached file is called “Shipping documents.zip” and according to Sophos, it contains a malicious executable detected as W32/AutoRun-BHY. Source: <http://news.softpedia.com/news/New-Wave-of-Fake-Amazon-Emails-Spreads-Malware-173495.shtml>

One-quarter of consumers have turned off their anti-virus software. Twenty-five percent of consumers surveyed by anti-virus software provider Avira turned off their anti-virus software because it was slowing down the computer, while 12 percent considered abandoning the Internet because of safety concerns. In addition, 63 percent of consumers have tried multiple anti-virus security products in a 1-year span on the same computer, according to the survey of 9,091 Avira customers worldwide. “It’s not surprising that consumers try multiple security products each year since everyone is trying to find the right security product which can effectively balance protection and a computer’s resource usage”, said a data security expert with Avira. “The scary take-away from this survey is that 25 percent of the respondents admitted to turning off their security products because they feel that it hurt the performance of the machine.” He said vendors must be careful not to overload anti-virus software with features that could have a significant effect on system performance. Anti-virus vendors should focus on offering products providing the minimum necessary protection, rather than protection “with all the whistles and bells” that users deactivate to use their computers. Source: <http://www.infosecurity-us.com/view/14755/onequarter-of-consumers-have-turned-off-their-antivirus-software/>

Symantec researcher spots C&C botnet toolkit in the wild. Security researchers from Symantec claim to have spotted a new crimeware toolkit being sold in the underground marketplace. The toolkit — known as Dream Loader — generates a Trojan exclusively used to distribute malware. According to a security researcher with Symantec, the toolkit is a command-and-control (C&C) botnet engine that is flagged up as Trojan.Karagany by Symantec's software. The malware generated by the toolkit is already circulating in the wild. The engine itself is said to come in a pack that contains both a builder to build an executable bot, as well as a Web interface to control all a hacker's bots by sending commands across the Internet. The security researcher said the pack — now into version 0.3 — is relatively new and seems to have originated from Russia. The first edition of the toolkit, he said, was discovered in November and is designed to be modular and load plugins. Source:

<http://www.infosecurity-magazine.com/view/14771/symantec-researcher-spots-cc-botnet-toolkit-in-the-wild/>

Gawker CTO outlines post-hack security changes. Gawker Media's CTO outlined a series of security changes designed to shore up the company's IT operations following an attack the week of December 12 that compromised up to 1.4 million accounts. The company was unprepared to respond to an attack where user data and passwords were posted to peer-to-peer file-sharing networks, said the CTO's December 17 e-mail memo to Gawker staff. A group called Gnosis claimed responsibility for the hack, which exploited a flaw in the source code of Gawker's Web servers. As a result, Gawker has done a security audit of the sites affected, including Lifehacker, Gizmodo, Gawker, Jezebel, io9, Jalopnik, Kotaku, Deadspin, and Fleshbot. Gawker is now mandating the use of SSL (Secure Sockets Layer) encryption for employees with company accounts using Google Apps. Also, if those employees have access to sensitive legal, financial or account data, two-factor authentication must be used. Gawker also will not allow employees to discuss sensitive information on chat applications, including AOL's Instant Messenger and Campfire. For users of its Web sites, the CTO wrote Gawker wants to move away from storing information such as e-mail and passwords and use systems such as OAuth. OAuth is an authentication protocol that allows people to use the same log-in information for multiple services and share data through an API (application programming interfaces). OAuth provides a token that grants access to different applications, which do not see users' original log-in credentials. It is being used now by Google, Twitter and Facebook, among other services. Gawker will also allow people to create a "disposable" account with its sites in order to leave comments. Source: http://www.computerworld.com/s/article/9201719/Gawker_CTO_outlines_post_hack_security_changes

NATIONAL MONUMENTS AND ICONS

(Utah) Zion National Park's scenic drive's stability in question. Zion National Park in Utah remains closed December 22 as a precaution due to rising river levels and the threat of damage to roadways, trails, and other infrastructure and potential threats to visitor safety. All visitors including guests at the Zion Lodge and Watchman Campground were evacuated safely on December 21. The park remained close pending an anticipated crest in the river. After this river surge, an assessment will be made of the condition and stability of sections of the Zion Canyon Scenic Drive and other park roads and facilities. Barring additional damage or safety concerns, the park anticipates reopening the Zion Lodge, Zion Canyon Scenic Drive, and Watchman Campground on December 23. Park trails will be assessed for damage and safety threats and reopened when it is deemed safe to do so. The Zion Mt. Carmel Highway, the east/west route through the park, will remain closed until damage caused by

UNCLASSIFIED

the current storm can be repaired. Source:

<http://www.thespectrum.com/article/20101222/NEWS01/101222026/Zion-National-Park-s-scenic-drive-s-stability-in-question>

(Wyoming) Avalanche danger high in NW Wyoming Mountains. New snow has raised the avalanche danger in northwestern Wyoming. The avalanche danger in higher elevations in the Bridger-Teton National Forest was listed as “high” December 20. The risk was considered moderate below 7,500 feet. One backcountry skier was swept up by an avalanche December 19 after crossing out of the Jackson Hole Mountain Resort. The Jackson Hole News & Guide reported that he was injured but was not buried in the slide. Nearly 1 foot of snow fell in Jackson, and wind gusts blew up to 50 mph on Rendezvous Mountain. The storm was expected to wind down December 21, although snow showers could linger through December 23. Source: http://billingsgazette.com/news/state-and-regional/wyoming/article_be1c409e-0c58-11e0-bd74-001cc4c03286.html

(Alaska) 4.5 magnitude earthquake hits Denali National Park. A 4.5 magnitude earthquake in Denali National Park and Preserve near Kantishna, Alaska, was felt December 17 in Talkeetna and Fairbanks, but no reports of damage were received, according to the Alaska Earthquake Information Center on the University of Alaska Fairbanks campus. The quake occurred at 3:01 a.m. and was centered 21 miles southwest of Kantishna. It was located at a depth of approximately 8 miles. Source: <http://newsminer.com/bookmark/10714175-4-5-magnitude-earthquake-hits-Denali-National-Park>

(California) Avalanche advisory issued in Sierra Nevada Mountains. The U.S. Forest Service (USFS) in Truckee, California, has issued an avalanche advisory due to significant snow levels, high winds and rain at higher elevations. The advisory will remain in effect until 8 a.m. December 20. USFS said the avalanche advisory impacts the Central Sierra Nevada Mountains between Yuba Pass on the North and Sonora Pass on the South. It applies only to backcountry areas outside established ski area boundaries. Avalanche danger is high on all Northwest, North and Northeast and Southeast aspects steeper than 30 degrees at all elevations. USFS recommended people travel around avalanche terrain including low elevation cut roads, and avoid steep hillsides. High avalanche hazards indicate that unstable snow exists in the back country. Source: <http://www.fox40.com/news/headlines/ktxl-avalanche-advisory-issued-in-s-121910,0,1155701.story>

POSTAL AND SHIPPING

For air cargo, a screening conundrum. Since the October discovery of explosives from Yemen hidden in ink cartridges on cargo planes, the \$50 billion freight business has seen little escalating security. Even in the midst of one of the air cargo industry’s busiest periods of the year, governments and aviation experts continue to struggle to come up with ways to strengthen cargo security without paralyzing a business essential to global trade. Cargo safety has suddenly emerged as one of the biggest topics in aviation security. Governments around the world have pledged to tackle the problem, while in Congress, lawmakers are calling for much tougher inspections of cargo. The cargo industry has resisted one idea: screening all cargo. It argues that such a step is impractical since most airports do not have the space to screen all the packages shipped each day. And some goods, including perishable products and medical supplies, may not survive a long wait at the airport to be screened. Air cargo can come from countless sources and comprises countless kinds of goods,

UNCLASSIFIED

UNCLASSIFIED

including fresh produce, medical supplies and electronic devices. The cargo industry itself is fragmented, too, with door-to-door shippers like DHL, United Parcel Service and FedEx; all-cargo airlines; and shipping companies that rent cargo space on passenger planes. Air cargo represents about 40 percent of the value of global trade. Source:

http://www.nytimes.com/2010/12/21/business/21cargo.html?_r=1&src=busln&pagewanted=all

(Alabama) FBI: Powder at Huntsville courthouse harmless. The FBI said a suspicious powder found at the federal courthouse in Huntsville, Alabama was deemed harmless after authorities shut down the building and surrounding streets for about 2 hours. FBI spokesman said the powder discovered in an envelope December 17 was not dangerous, but tests are still being conducted to determine what the substance is. The incident caused police to close down two streets around the courthouse, and a hazardous materials team set up a decontamination station. A woman who found the envelope was taken to a hospital as a precaution. Authorities would not say who the envelope containing the powder was mailed to. Source: <http://www.wrcbtv.com/Global/story.asp?S=13707749>

PUBLIC HEALTH

GAO: HHS does not have plan for IT pandemic surveillance. The Health and Human Services (HHS) Department has not developed a strategic plan for a national electronic network for public health situational awareness four years after being told to do so by Congress, according to a new report from the Government Accountability Office (GAO). The department has made progress on developing related systems — such as those for biosurveillance, health data exchange, and public health information sharing — but has not made progress on a comprehensive plan for situational awareness, GAO said in the December 17 report. “HHS has not defined a comprehensive strategic plan that identifies goals, objectives, activities, and priorities and that integrates related strategies to achieve the unified electronic nationwide situational awareness capability required by PAHPA,” the GAO report states. The legislation was intended to meet the need for efficient sharing of near-real-time information during a public health emergency. HHS was supposed to coordinate with state and local agencies to create a strategy and a national network for monitoring public health electronically in near-real time. Source: <http://homelandsecuritynewswire.com/gao-hhs-does-not-have-plan-it-pandemic-surveillance>

(Indiana) Urey school absences blamed on virus. About 40 percent of students missed class December 22 at a St. Joseph County, Indiana middle school. Administrators are blaming most of the absences on a norovirus. The illness also spread to many teachers at Urey Middle School in Walkerton. One hundred twenty-five of the school’s 300 students were out December 22. The St. Joseph County Health Department believes a norovirus, which is similar to the stomach flu but more contagious, is the culprit. Symptoms are vomiting and diarrhea; the virus lasts 24 to 48 hours. The Health Department says young kids are the biggest risk because they can get dehydrated. Holiday break starts for Urey Middle School today so the school did not need to make any decision about canceling classes. However, a cleaning crew would be at the school December 23 to disinfect the building. Source: <http://www.southbendtribune.com/article/20101223/News01/12230303/-1/googleNews>

UNCLASSIFIED

TRANSPORTATION

(Illinois) 1 in 13 local bridges ‘structurally deficient’. There are 293 structurally deficient bridges in the Chicago, Illinois metropolitan region — Cook, DuPage, Kane, Lake, McHenry, and Will counties, according to state and federal data. Those counties contain 3,691 bridges in all. More than half of the deficient bridges — 153 — are in Cook County, 78 of them in the suburbs. Will County has 45 deficient bridges. Kane County is home to 27. DuPage County has 23. Lake County’s tally is 23. And McHenry County holds 22. Drivers can not always tell which bridges are bad. Significant defects to a bridge may not be noticeable to the naked eye, Illinois Department of Transportation (IDOT) officials said. Structural issues may occur within the bridge and may not appear outwardly as a flaw, experts said. Source: <http://www.dailyherald.com/article/20101222/news/712229721/>

(Colorado) ‘Epic’ mountain snow continues; mild and breezy in metro Denver. On December 20, U.S. 50 over Monarch Pass, Colorado was closed due to numerous snow slides. U.S. 6 over Loveland Pass was closed because of adverse conditions. That created delays at the Eisenhower Tunnel when traffic was halted to allow vehicles carrying hazardous materials to pass through the tunnel. Winter storm warnings continued for the mountains as a 6-day blockbuster winter storm is underway in Colorado’s high country. It could be one of the biggest mountain snowstorms ever in Colorado. Locales above 9,000 feet could expect storm snowfall grand totals by December 25 of 4 to 8 feet, and places below 9,000 feet could expect 1 to 2 feet of total snow. This winter storms stretches from the Gulf of Alaska all the way south in California, through Las Vegas, Nevada into Colorado, and northeast into Minnesota. There were also delays on I-70 for avalanche control west of the Eisenhower Tunnel and at Vail Pass, as well as on U.S. 40 at Berthoud Pass also for avalanche control. Source: <http://www.kdvr.com/news/kdvr-heavy-mountain-snow-continues-121910,0,4325576.story>

WATER AND DAMS

EPA likely to toughen drinking water regulations. The EPA Administrator says the Environmental Protection Agency is concerned about the prevalence in drinking water of the chemical known as chromium 6. Chromium 6 was discovered in drinking water in 31 cities across the country. Madison, Wisconsin was among the five cities with the highest levels of the carcinogen. The Administrator says the EPA is likely to tighten drinking water standards to address potential health risks of the chemical. Source: http://www.wuwm.com/programs/news/view_news.php?articleid=7452

Congress moves to reduce lead in drinking water. Congress December 17 sent the U.S. President a bill that would significantly reduce exposures to lead in drinking water. The House approved the bill on a 226-109 vote. The Senate approved it earlier on a voice vote. The bill would set federal standards for levels of permissible lead in plumbing fixtures that carry drinking water, with allowable lead content going from the current federal level of as much as 8 percent to 0.25 percent. It limits the amount of lead that can leach from plumbing into drinking water. A U.S. Representative from Pennsylvania said the new standards would nearly eradicate lead in faucets and fixtures. He cited U.S. Environmental Protection Agency estimates that lead from these sources contribute to up to 20 percent of human exposure. The bill becomes effective 36 months after it is signed into law. It would prohibit manufacturers and importers from selling plumbing fixtures that don’t meet the new

UNCLASSIFIED

standards. Almost all opposition came from Republicans, such as a Representative from Florida who questioned the necessity of passing a federal law when major producers of faucets are already making safer equipment and some states are imposing their own tough standards. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/17/AR2010121705270.html>

Chromium-6 is widespread in U.S. tap water. Tests commissioned by the Environmental Working Group (EWG) detected carcinogenic hexavalent chromium in 31 of 35 tap water samples — 89 percent — collected in cities across the country as described in the report, released December 20. EWG targeted a mix of large cities and some smaller ones where testing by local water utilities had previously detected potentially significant amounts of “total chromium.” This less specific measurement includes trivalent chromium, an essential mineral that regulates glucose metabolism, as well the cancer-causing hexavalent form, also called chromium-6. Chromium widely contaminates U.S. tap water. Hexavalent chromium (or chromium-6) gets into water supplies after being discharged from steel and pulp mills as well as metal-plating and weather-tanning facilities. It can also pollute water through erosion of soil and rock. In California, the only state that requires water utilities to test for hexavalent chromium, the state’s Environmental Protection Agency (California EPA) has proposed a “public health goal,” or maximum safe concentration, of 0.06 parts per billion (ppb) in tap water to protect against excess cancer risk. Nationally, samples from 25 cities tested by EWG had levels of hexavalent chromium higher than the safe limit proposed in California. EWG recommended the U.S. EPA set a legal limit for hexavalent chromium in drinking water as quickly as possible, and require all water utilities to test for it. Source: <http://www.ewg.org/chromium6-in-tap-water/findings>

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: 701-328-8175
State Radio: 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED